REMARKS

The Office Action dated July 21, 2008, has been received and carefully noted. The above amendments to the specification and claims, and the following remarks, are submitted as a full and complete response thereto.

By this Response, claims 1-2, 5-10, and 12 have been amended to more particularly point out and distinctly claim the subject matter of the present invention. Claims 15-29 have been added. No new matter has been added. Support for the above amendments is provided in the Specification at least on page 4, line 5, to page 9, line 3. Accordingly, claims 1-12 are currently pending in the application, of which claims 1, 12, 15, 20, and 25 are independent claims.

In view of the above amendments and the following remarks, Applicants respectfully request reconsideration and timely withdrawal of the pending rejections to the claims for the reasons discussed below.

Drawing Objection

The Office Action objected to the drawings under 37 C.F.R. 1.84(p)(4), alleging that reference numerals, "1" and "2" have both been used to designate "hub" in the disclosure of the Specification. In particular, the disclosure of the Specification recites, "Hub 1 also includes a link security controller 15" (See page 5, lines 27-28). The Office Action indicated that "Hub 1" on page 5 on line 27 should be changed to "Hub 2."

Accordingly, Applicants have amended the disclosure of the Specification at page 5, lines 27-28, as follows: "~~Hub 1~~ Hub 2 also includes a link security controller 15," rendering the objection to the drawings under 37 C.F.R. § 1.84(p)(4) moot.

Therefore, Applicants respectfully request withdrawal of the objection to the drawings under 37 C.F.R. §1.84(p)(4), and respectfully submit that the drawings are in condition for issuance.

Abstract

The Office Action objected to the Abstract, stating that the abstract should be on a separate sheet, *i.e.*, without a drawing/title or should not be a PCT first page.

Accordingly, Applicants have amended the Abstract to comply with the requirements of MPEP §608.01(b) and 37 C.F.R. §1.72. Therefore, Applicants respectfully request withdrawal of the objection to the Abstract, and respectfully submit that the Abstract is now in condition for issuance.

Claim Objections

The Office Action objected to claims 1, 8-9, and 12 because of minor informalities. Specifically, the Office Action indicated that claim 1 at line 7 should be amended from "addresses allocated" to "link-level addresses allocated" to provide sufficient antecedent basis. Further, the Office Action indicated that claim 9 at line 2, and claim 12 at line 6 should be similarly amended. Further, the Office Action indicated

that claim 8 requires amendment to clarify the recited features for the data distribution unit.

Accordingly, Applicants have amended claims 1, 8-9, and 12 to more particularly point out and distinctly claim the subject matter of the present invention, rending the objection to claims 1, 8-9, and 12 moot.

Therefore, Applicants respectfully request withdrawal of the objections of claims 1, 8-9, and 12, and respectfully submit that claims 1 and 12, and the claims that depend therefrom, are now in condition for allowance.

Claim Rejections under 35 U.S.C. §103(a)

Claims 1-7, 9, and 12

The Office Action rejected claims 1-7, 9, and 12 under 35 U.S.C. §103(a) as being allegedly unpatentable over Elliott, *et al.* (U.S. Patent No. 5,276,813) ("Elliott") in view of Lyle (U.S. Patent No. 6,886,102) and Nikander (Great Britain Patent No. GB 2367986). Applicants respectfully submits that the claims recite subject matter that is neither disclosed nor suggested in the combination of Elliot, Lyle, and Nikander.

Claim 1, upon which claims 2-11 depend, recites a communication system. The communication system includes a plurality of communication nodes connected by a data link, and a communication controller configured to allocate link-level addresses to the communication nodes. The communication nodes may be identified for communications over the data link. The communication controller is further configured to change from

time to time the link-level addresses allocated to each communication node and to transmit the newly allocated link-level address to a respective communication node in an encrypted form.

Claim 12 recites a method for communicating data in a communication system. The communication system includes a plurality of communication nodes connected by a data link and a communication controller. The method includes allocating link-level addresses to the communication nodes whereby the communication nodes may be identified for communications over the link. The method further includes changing from time to time the link-level addresses allocated to each communication node, and transmitting the newly allocated link-level address to a respective communication node in an encrypted form.

Applicants respectfully submit that certain embodiments of the present invention provide non-obvious advantages. Specifically, certain embodiments of the present invention relate to a communication system including a plurality of communication nodes connected to a data link. The communication controller allocates link-level addresses to the communication nodes, whereby the communication nodes may be identified for communications over the data link. The communication controller changes from time to time the link-level addresses allocated to each communication node and transmits the newly allocated link-level address to a respective communication node in an encrypted form to protect transferred data from being access by an unauthorized person.

As will be discussed below, the combination of Elliot, Lyle, and Nikander would fail to disclose or suggest each and every element recited in claims 1-7, 9, and 12, and therefore fails to provide the advantages and the features discussed above.

Elliot is directed to a method for acquiring addresses in an input/output system. Elliot describes a computer I/O system including a plurality of link-level facilities and a dynamic switch having a plurality of ports. Each link-level facility is attached to one of the ports. As each of the link-level facility comes on line, the link-level facility sends an acquire link address (ALA) frame and waits for a response (ACK) frame. The ALA frame may be addressed to a general to-whom-it-may-concern address and have a source address of who-am-I. When receiving an ALA frame, the dynamic switch returns an ACK frame having a unique link address assigned to the sender of the ALA frame. Provision is made for determining if there is a dynamic switch present, or, if the link-level facilities are connected together by a static connection through the dynamic switch for the link-level facility of a channel to assign the unique link addresses (Elliot, Abstract; col. 2, line 47, to col. 3, line 32).

Lyle is directed to a system and method for protecting a computer network against denial of service attacks. In particular, Lyle describes a system and method for determining whether a sender seeking to send a message to a receiving computer system via a network is an authorized sender. A request to communicate is received from the sender, and a number N1 is selected. A hash value for the number N1 is calculated,

whereby the hash value is sent to the sender (Lyle, Abstract; col. 2, line 42, to col. 3, line 2).

Nikander is directed to an IP network authorization using a coded interface identifier part of an IP address. Nikander describes a method for verifying that a host coupled to an IP network is authorized to use an IP address for which the host claims as its own. The IP address includes a routing prefix and an identifier part. The method includes receiving from the host one or more components, applying a one-way coding function to each component and/or derivatives of each component. The method further includes comparing the result or a derivative of the result against the interface identifier part of the IP address. If the result or the derivative matches the interface identifier, the host is assumed to be authorized to use the IP address . If the result or the derivative does not match the interface identifier, the host is not assumed to be authorized to use the IP address. Nikander also describes a method for authenticating a public key and a method for generating the interface identifier part of an IP address (Nikander, Abstract).

Assuming *arguendo* that the teachings of Elliott could be combined with the teachings of Lyle and the teachings of Nikander, the combination of Elliot, Lyle, and Nikander would fail to disclose or suggest each and every element recited in claims 1 and 12. In particular, the combination of Elliot, Lyle, and Nikander would fail to disclose or suggest, at least, "wherein the communication controller is further configured to change from time to time the link-level addresses allocated to each communication node and to transmit the newly allocated link-level address to a respective communication node in an

encrypted form," as recited in claim 1 (emphasis added), and similarly recited in claim 12.

The Office Action alleged that Elliott discloses every feature recited in claims 1 and 12 with the exception of the communication controller being configured to change from time to time the link-level addresses allocated to each of a plurality of communication nodes and to transmit the newly allocated link-level address to a respective communication node in an encrypted form (See Office Action on page 4). The Office Action alleged that Lyle, at column 30, lines 8-55, and Nikander, at column 5, lines 24-29, and at column 6, line 16, to column 7, line 7, cure the deficiencies of Elliott. However, a review of these passages of Lyle and Nikander demonstrate that both Lyle and Nikander fail to cure the deficiencies of Elliott.

Rather, as previously noted above, Nikander merely relates to the malicious use of IP addresses in order to deny a node access or to re-route data packets intended for a node to a malicious party. In order to solve this problem, Nikander discusses an encryption of the IP address. Using the arrangement described in Nikander, a malicious third party could intercept transmissions that are addressed to other nodes and store them for a later decryption. Once the address has been decrypted, the malicious third party will be able to obtain valuable ancillary information. Hence, Nikander merely discusses transmitting an allocated address to a respective node in encrypted form. Accordingly, Nikander fails to mention or suggest that a "communication controller is further configured to change from time to time the link-level addresses allocated to each communication node and to

transmit the newly allocated link-level address to a respective communication node in an encrypted form," as recited in claim 1 (emphasis added), and similarly recited in claim 12.

Applicants further respectfully submit that Lyle fails to cure the deficiencies of Elliott and Nikander. Rather, Lyle describes a system and method for protecting a computer network or sub-network against an attack from an exterior source. Accordingly, Lyle focuses on monitoring nodes within the network or sub-network for an external attack. The network or sub-network is disposed behind a firewall. If it is suspected that the network or sub-network is under attack, then the handoff receiver port and/or IP address of the handoff receiver node at the firewall are changed.

Therefore, Lyle is primarily concerned with protecting a network or sub-network against attack. The security system of Lyle fails to protect communications outside the domain of the network or sub-network that it is specifically directed at monitoring, although the security system described in Lyle can pass security information to other systems.

In contrast, certain embodiments of the present invention are not directed at protecting a specific network or sub-system against attack through a firewall, but rather they are directed at protecting a communication against someone listening in on the communication over the entire length of the communication. In order to accomplish this objective, certain embodiments of the present invention provide for changes from time to time to the link-level addresses allocated to each of a plurality of communication nodes

linked by a data link. Thus, by identifying the plurality of communication nodes of a data link and changing from time to time the addresses allocated to each of the plurality of communication nodes involved in the data link, the data link may be protected from intrusion.

Therefore, Lyle is specifically related to protecting a network or sub-network against an external attack. In the teachings of Lyle, the system allows for someone to listen in on a communication sent from a sending system that has not yet entered the receiving system. Thus, data sent from the sending system is not protected. Only the receiving system is protected from an external attack.

Whereas, certain embodiments of the present invention are related to protecting a data link along the length of the data link. The plurality of communication nodes are identified and the link-level addresses for each of the communication nodes are changed from time to time to protect data being sent along the data link.

Accordingly, Lyle fails to disclose or suggest, at least, "that a "communication controller is further configured to change from time to time the link-level addresses allocated to each communication node and to transmit the newly allocated link-level address to a respective communication node in an encrypted form," as recited in claim 1 (emphasis added), and similarly recited in claim 12.

Accordingly, the combination of Elliot, Lyle, and Nikander would fail to disclose or suggest each and every element recited in claims 1 and 12.

Claims 2-7 and 9 depend from claim 1. Accordingly, claims 2-7 and 9 should be allowable for at least their dependency upon an allowable base claim, and for the specific limitations recited therein.

Accordingly, Applicants respectfully request withdrawal of the rejections of claims 1-7, 9, and 12 under 35 U.S.C. §103(a) and respectfully submit that claims 1 and 12, and the claims that depend therefrom, are in condition for allowance.

Claim 8

The Office Action rejected claim 8 under 35 U.S.C. §103(a) as being allegedly unpatentable over Elliott in view of Lyle and Nikander, and further in view of Laxman, *et al.* (U.S. Patent No. 2003/0018804) ("Laxman"). Applicants respectfully submits that the claims recite subject matter that is neither disclosed nor suggested in the combination of Elliot, Lyle, Nikander, and Laxman.

Elliott, Lyle, and Nikander were discussed above. Laxman is directed to a method and apparatus for deriving a standard MAC address from a physical location (Laxman, Abstract; paragraphs [0014]-[0017]).

As previously noted above, the combination of Elliott, Lyle, and Nikander would fail to disclose or suggest each and every element recited in claim 1. Laxman fails to cure the deficiencies of Elliott, Lyle, and Nikander. In particular, Laxman fails to disclose or suggest, at least, "wherein the communication controller is further configured to change from time to time the link-level addresses allocated to each communication

node and to transmit the newly allocated link-level address to a respective communication node in an encrypted form," as recited in claim 1 (emphasis added).

Accordingly, the combination of Elliott, Lyle, Nikander, and Laxman would fail to disclose or suggest each and every element recited in claim 1. Claim 8 depends from claim 1. Accordingly, claim 8 should be allowable for at least its dependency upon an allowable base claim, and for the specific limitations recited therein.

Accordingly, Applicants respectfully request withdrawal of the rejection of claim 8 under 35 U.S.C. §103(a) and respectfully submit that claim 1, and the claims that depend therefrom, are in condition for allowance.

Claims 10-11

The Office Action rejected claims 10-11 under 35 U.S.C. §103(a) as being allegedly unpatentable over Elliott in view of Lyle and Nikander, and further in view of Woundy (U.S. Patent No. 6,009,103). Applicants respectfully submits that the claims recite subject matter that is neither disclosed nor suggested in the combination of Elliot, Lyle, Nikander, and Woundy.

Elliott, Lyle, and Nikander were discussed above. Woundy is directed to a method and apparatus for an automatic allocation of resources in a network (Woundy, Abstract).

As previously noted above, the combination of Elliott, Lyle, and Nikander would fail to disclose or suggest each and every element recited in claim 1. Woundy fails to cure the deficiencies of Elliott, Lyle, and Nikander. In particular, Woundy fails to

disclose or suggest, at least, "wherein the communication controller is further configured to change from time to time the link-level addresses allocated to each communication node and to transmit the newly allocated link-level address to a respective communication node in an encrypted form," as recited in claim 1 (emphasis added).

Accordingly, the combination of Elliott, Lyle, Nikander, and Woundy would fail to disclose or suggest each and every element recited in claim 1. Claims 10-11 depend from claim 1. Accordingly, claims 10-11 should be allowable for at least their dependency upon an allowable base claim, and for the specific limitations recited therein.

Accordingly, Applicants respectfully request withdrawal of the rejections of claims 10-11 under 35 U.S.C. §103(a) and respectfully submit that claim 1, and the claims that depend therefrom, are in condition for allowance.

CONCLUSION

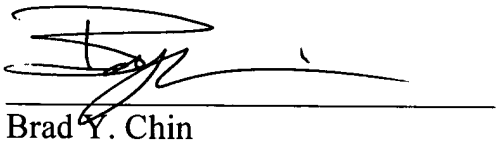
In conclusion, Applicants respectfully submit that Elliott, Lyle, Nikander, Laxman, and Woundy, whether taken individually or in combination, fail to disclose or suggest each and every element recited in claims 1-12 and 15-29. The distinctions previously noted are more than sufficient to render the claimed invention non-obvious. It is therefore respectfully requested that all of claims 1-12 and 15-29 be allowed, and this present application be passed to issuance.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by

telephone, Applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Brad Y. Chin
Attorney for Applicants
Registration No. 52,738

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

BYC:dlh

Enclosures: Additional Claim Fee Transmittal
Check No. 019816